sāflink®
CORPORATION

PROTECTING YOUR ENTERPRISE THROUGH SECURE AUTHENTICATION™

COMPUTER NETWORKS
PHYSICAL FACILITIES
APPLICATIONS
MANUFACTURING AUTOMATION SYSTEMS
TIME & ATTENDANCE SYSTEMS
IDENTITY ASSURANCE MANAGEMENT™

Breakout Session 2
Elements of Secure Biometric-Based Authentication Systems

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Workshop on Biometrics and Remote E-Authentication Over Open Networks

Objective

- Determine: How should biometrics play a role at each of the 4 ‘identity authentication assurance levels’

Level	Confidence in Asserted Identity’s Validity
1	Little or none
2	Some
3	High
4	Very High

Currently Specified

- Biometric methods are widely used to authenticate individuals who are physically present at the authentication point, for example for entry into buildings.
- Biometrics do not constitute secrets suitable for use in the conventional remote authentication protocols addressed in this document.
- In the local authentication case, where the claimant is observed and uses a capture device controlled by the verifier, authentication does not require that biometrics be kept secret.
- The use of biometrics to "unlock" conventional authentication tokens and to prevent repudiation of registration is identified in this document.

Questions to be answered

- What architectures are appropriate?
- What properties of the biometric components are required?
- What issues need to be addressed?
- How can cryptographic and other security mechanisms be used in conjunction with biometrics to provide a robust authentication solution?
- What architectures provide the features needed for use at each level?
- What criteria should be used to rate these architectures?

Questions (cont’d)

- How does the fact that biometrics are not secrets affect the way they are used?
- What role do certifications play?
- What differences exist between access by employees and the citizenry?
- Can/should FAR requirements be identified for each level?

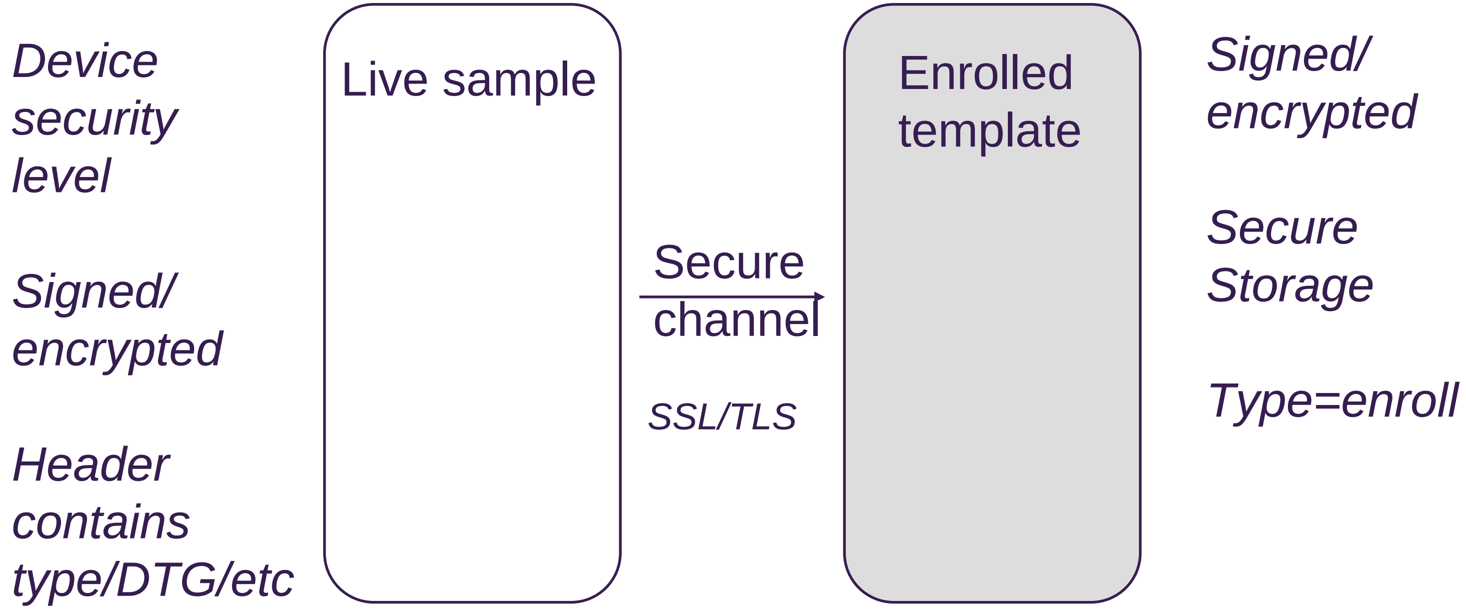
Architectures

- Basic considerations
  - Where is the biometric enrollment data stored?
  - Where is the matching performed?
  - How is the data protected during storage & transmission?
  - What protections exist on the system as a whole & on the individual components?
  - What protections are assumed for a physical token and do these same protections apply to a biometric device?
  - What are the threats and risks, really? What can we assume about an attacker at each level?
  - Is local/token matching always better than server based matching? Why?

Biometrics as an authentication token

- 800-63 precludes this (even at Level 1)
  - Tokens are always secrets
  - Biometrics are not secrets
  - ergo, biometrics cannot be used as tokens

- Analogy between biometrics & the public key?



Device security level

Signed/ encrypted

Header contains type/DTG/etc

Live sample

Secure channel

SSL/TLS

Enrolled template

Signed/ encrypted

Secure Storage

Type=enroll

Authentication Tokens

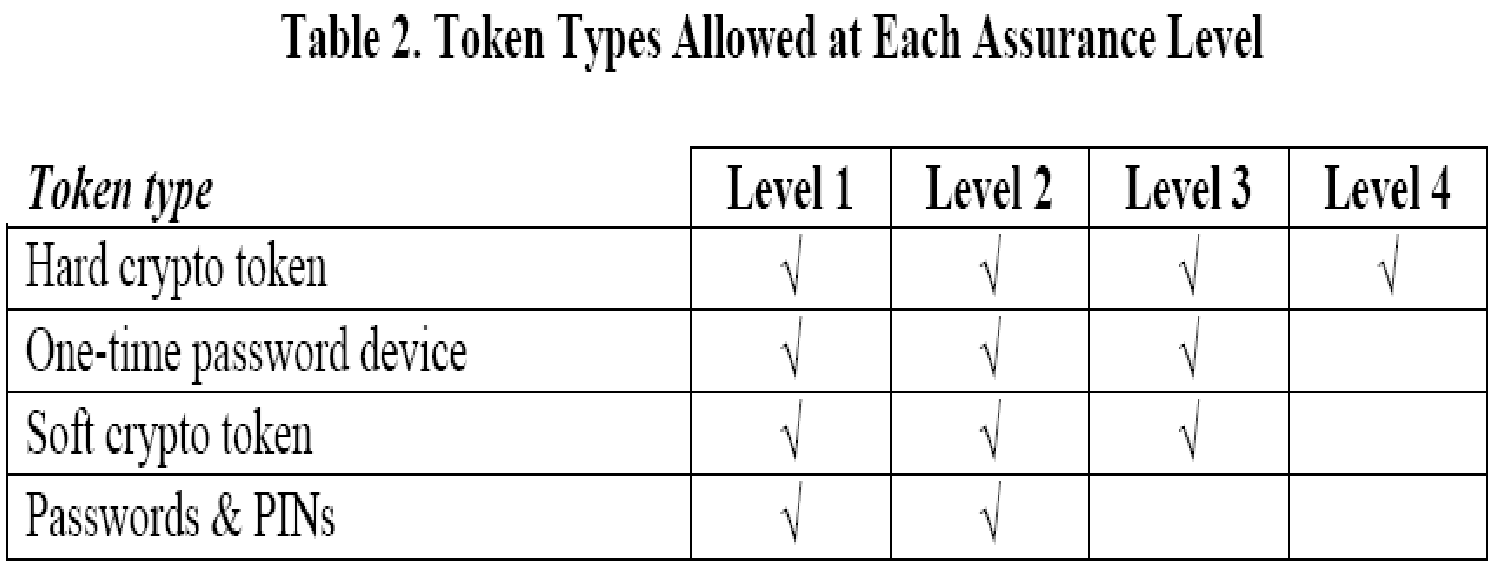


Table 2. Token Types Allowed at Each Assurance Level

Token type	Level 1	Level 2	Level 3	Level 4
Hard crypto token	√	√	√	√
One-time password device	√	√	√	
Soft crypto token	√	√	√	
Passwords & PINs	√	√		

Potential issues to be addressed

- Secrecy
- Randomness
- Revocation
- Spoofing and other attacks
- Non-repudiation
- Public review
- Privacy considerations

- What issues are unique to biometrics?

- How does the introduction of biometrics alter or place additional requirements on the underlying security infrastructure?

More Questions

- How can biometric data be compromised?
  - What would it take to do this?

- What could it be used for if obtained?
  - What existing security mechanisms are in place to protect against this?
  - What new mechanisms are needed?

800-63 does a good job of identifying potential attacks, but does not look at attacks against a biometric specifically.

Comparison of technologies

	Strengths	Weaknesses
Passwords One-time passwords Random passwords Soft crypto token Symmetric Asymmetric Hard token Physical token Biometric …		

Time permitting & if deemed worthwhile

Problem to be solved

- Remember:
  - "security and privacy of sensitive unclassified information"
- Example scenarios from OMB M-04-04:
  - Level 1:
    - an individual applies to a Federal agency for an annual park visitor's permit
  - Level 2:
    - A beneficiary changes her address of record through the Social Security web site.
  - Level 3:
    - A patent attorney electronically submits confidential patent information to the US Patent and Trademark Office.
  - Level 4:
    - A law enforcement official accesses a law enforcement database containing criminal records.

Discussions

- Impossible to avoid discussion of threats and countermeasures, but will attempt to not delve too deeply into this
  - Subject of separate breakout session
- However, it is difficult to discuss a security architecture in isolation from the threats against it.

Approach

- Begin with review of how biometrics are characterized and utilized within the current 800-63 document
  - Perhaps challenging some underlying assumptions & paradigms
- Brainstorm & suggest ways that biometrics can be used effectively
- Identify limitations, constraints, and requirements to how they should be used
- Determine what requirements on the system as a whole are needed to allow biometrics to be integrated appropriately

End Goal

- Prepare a recommendation on use of biometrics at each of the 4 levels, providing:
  - A general description of the mechanism
  - Identification of requirements for use
  - An example use case scenario
  - Identification of components
- Recommend contents for a Biometric Appendix (?)

Ancillary Goals

- Identify areas for additional research
- Provide recommendations for:
  - Standards – existing/new
  - Testing & certification
- Provide recommendations for improvements to industry:
  - Biometric component vendors
  - System integrators / solution providers

Keep in Mind

- Perfection is neither achievable nor required
- Our job is to figure out how good is has to be

  and
- How to make it so.

The Beginning

Catherine J. Tilton
SAFLINK Corp.
1875 Campus Commons Dr, Suite 301
Reston, VA 20191

ctilton@saflink.com
703-547-0404
Cell 703-472-5546
Fax 703-547-0399